CJIS Information Letter   **February 29, 2016**

Computer security upgrade will affect all CJIS Division systems accessed through the Internet

Beginning April 1, 2016, a computer security upgrade will affect all CJIS Division systems that agencies access through the Internet.

Background

All agencies that access CJIS Division systems via the Internet do so through a Trusted Internet Connection (TIC) and, to date, may use versions 1.0, 1.1, or 1.2 of the Transport Layer Security (TLS) to securely send data to the division electronically. The TIC monitors existing public Internet connections on government networks and limits the number of public Internet access points so data can be analyzed more effectively. The TLS is an encryption protocol that ensures privacy between communicating applications and Internet users.

Effective April 1, 2016, the CJIS Division's staff will disable all TLS versions below 1.2 and will no longer support TLS versions 1.0 and 1.1 because those versions have vulnerabilities.

Any Web browsers or security devices that do not have TLS version 1.2 enabled will no longer be able to access CJIS Division systems. Connections from networks with Web proxies or other security devices that do not support TLS version 1.2 may also affect a user's ability to access DOJ Web sites and Web services.

What systems are affected?

This affects **all** CJIS Division systems that agencies access via the Internet, including the:
- ❖ National Crime Information Center (NCIC)
- ❖ National Data Exchange (N-DEx)
- ❖ Next Generation Identification (NGI)
- ❖ Interstate Identification Index (III)
- ❖ Uniform Crime Reporting (UCR) Program
- ❖ Law Enforcement Enterprise Portal (LEEP)
- ❖ National Instant Criminal Background Check System (NICS) (including Echeck).

What systems are not affected?

This change does not impact your ability to send or receive e-mails from leo. gov or ic.fbi.gov addresses, and it does not affect your ability to view or download information from the fbi.gov Web site.

Also, this does not affect any agency that accesses the division's systems through the CJISWAN (Wide Area Network), which uses telephone lines or other devices to connect computers.

What types of devices does this affect?

This change affects all Internet-enabled devices, including all desktop and laptop computers as well as personal electronic devices, such as iPads and Bureau-issued smartphones.

How can I find out if my browser is compatible?

To determine software compatibility, you can reference lists available on the Internet that document the compatibility of Web browsers and application platforms like Java and .Net.

In addition, the CJIS Division has created a site for agencies to test their ability to access CJIS Division systems. To determine if your agency's computer security uses or is compatible with version 1.2 of the TLS, you may go to <www.cjis.gov> or <https://test. cjis.gov> and follow the prompts to conclude the agency's readiness.

If you choose to access <www.cjis.gov>, click on the ATTENTION:TLS Browser Compatibility Test link. (See the next page.)

If you opt to go to <https://test.cjis.gov>, simply look for the following information in the fourth paragraph on that page:

> ✓ **TLS 1.2 Compatible Browser**
> Your web browser successfully connected to this website which is available only through a TLS 1.2 connection. Your operating system and web browser are ready for the new security settings which will go into affect April 1, 2016 and no further work by you is neccessary to be ready for the increase in security

This notice indicates that the user's computer has a browser that is compatible with TLS version 1.2, and you do not need to take any additional steps.
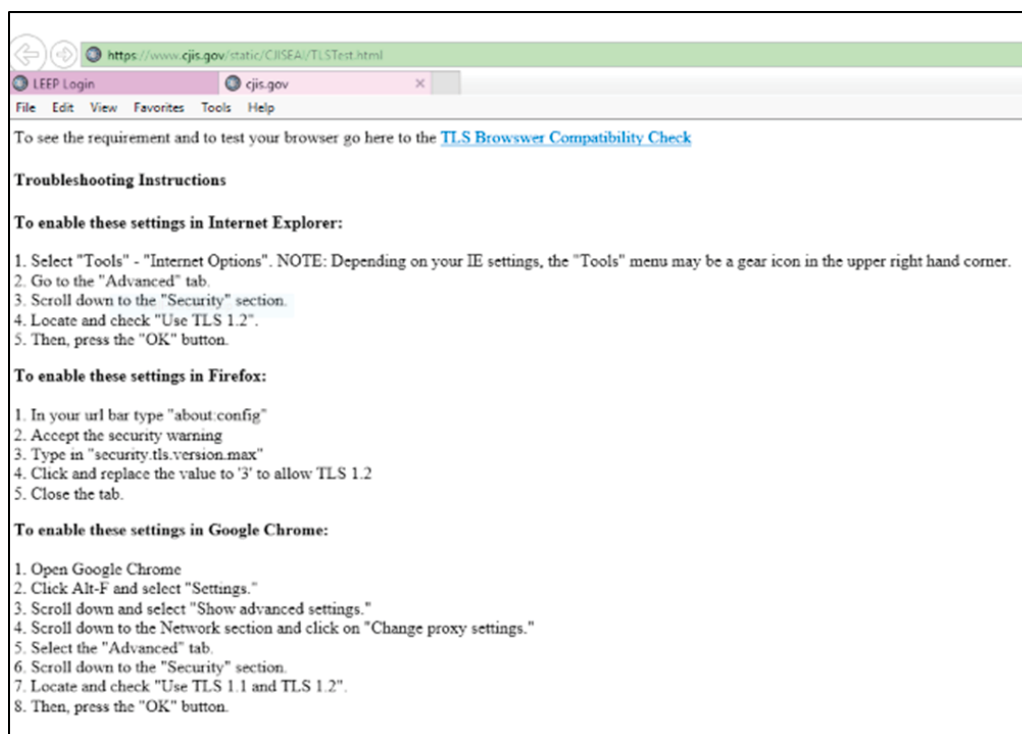
However, if you go to <www.cjis.gov>, click on the ATTENTION:TLS Browser Compatibility Test link, or go to <https://test.cjis.gov> and see the following information,
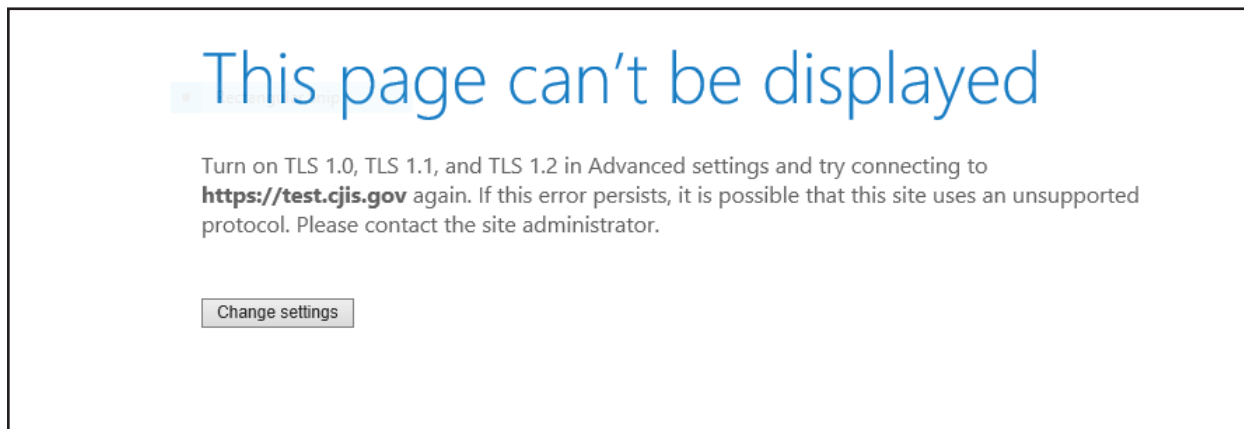
the browser is not compatible with TLS version 1.2,. You should go to <www.cjis.gov>, click on the Go to the TLS troubleshooting page link, and follow the onscreen instructions for your agency's Internet browser.

You will see the following screen:

Why is this change happening?

An executive order from the Office of Management and Budget (OMB) released on June 8, 2015, (OMB Memorandum M-15-13) requires that all publicly accessible federal Web sites and Web services provide services only through secure connections. The National Institute of Standards and Technology strongly recommended that agencies migrate to the TLS version 1.2 (Special Publication 800-52 revision 1 from April 2014).

Future CJIS Division systems or Web sites will require TLS version 1.2 to access the information. Agencies will be notified of any future upgrades to a more advanced version of the TLS.

Where do I go if I have questions?

For questions about how the change affects access to the various CJIS systems:

❖ For NCIC, contact Johnna McDonald by telephone at (304) 625-4543 or e-mail her at <johnna.mcdonald@ic.fbi.gov>.

❖ For N-DEx, contact Joshua Paul Binegar by telephone at (304) 625-5314 or e-mail him at <joshua.binegar@ic.fbi.gov>.

❖ For NGI, contact the Biometric Services Section's Customer Service Group (CSG) by telephone at (304) 625-5590 or contact the CSG by e-mail at <CK_CSG@ic.fbi.gov>. For submitting latent fingerprints, contact the Latent and Forensic Support Unit by telephone at (304) 625-5868.

❖ For LEEP, contact the FBI's Support Center at 1-(800) 334-4536.

❖ For NICS, contact R. Marc Chamberlain by telephone at (304) 625-7544 or e-mail him at <marc.chamberlain@ic.fbi.gov>.

CJIS Information Letters available on the Law Enforcement Enterprise Portal

CJIS Information Letters are available via the Internet on the LEEP at <https://leo.cjis.gov/leoContent/lesig/cjis/general_information/newsletters/information_letter/> or by clicking on:

❖ SIGs
❖ By Access Type
❖ Unrestricted
❖ CJIS
❖ General Information tab
❖ Newsletters and Reports
❖ CJIS Informational Letters

If you have questions concerning access to the LEEP, contact the LEEP Help Desk by telephone at (888) 334-4536.

In addition, this _CJIS Information Letter_ will be sent to CJIS Security Officers, State Information Bureaus, and Compact Council members via e-mail.